ABSTRACT

A policy agent of a network performs an out-of-band user authentication process to verify the identity of a user of a client computer and associates the network data received from the client compute with the user. When the client computer initiates a network data connection to or through the policy agent, the policy agent sends an encrypted challenge to the client computer. The challenge is encrypted with a private key of the policy agent. When the client computer received the challenge, it decrypts the challenge and prepares a message digest value based on the challenge and the network data sent by the user. The message digest value is then encrypted with the private key of the user to form a response, and the response is sent to the policy agent. The policy agent decrypts the response with the public key of the user to obtain the message digest value and calculates a digest value based on the challenge and the received network data. The policy agent then compares the calculated digest value with the decrypted digest value. A match between the two digest values indicates that the user is successfully authenticated, and that the received network data is associated with the user. The policy agent may then apply network policies based on the credentials of the authenticated user.